National Infrastructure Protection Center CyberNotes

Issue #2000-11 *June 5, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 18 and June 2, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures. For more information on this effort, see http://cve.mitre.org.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cayman[1] *Patch now available.*[2]	**220-H DSL Router 1.0, GatorSurf 5.5Build R0, 5.3Build R2, 5.3Build R1**	**A Denial of Service vulnerability exists when a large username or password string is sent to the Cayman HTTP admin interface.**	**No workaround or patch available at time of publishing.** *Patch available at:* ftp://www.cayman.com/pub/gatorsurf/3220/c8a550R1.COS	**DSL Router Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[1] Bugtraq, May 5, 2000.
[2] Bugtraq, May 23, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cayman[3]	3220-H DSL Router 1.0, GatorSurf 5.5Build R1, 5.5Build R0, 5.3Build R2, 5.3Build R1, GatorSurf 5.3	A "ping of death" vulnerability exists when an oversized ICMP echo request is sent to the router.	No workaround or patch available at time of publishing.	Cayman 3220H DSL Router "ping of death"	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco[4]	TACACS+ Server Developer's Kit	Several vulnerabilities exist in the TACACS+ protocol. The discussion can be read at http://www.openwall.com/advisories/	Cisco has publically released a statement that no patches will be released. An unofficial workaround exists at: http://www.openwall.com/advisories/	Cisco TACACS+ Multiple Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Cobalt[5]	RaQ2, RaQ3 FrontPage	A vulnerability in the FrontPage extensions on the Cobalt RaQ2 and RaQ3 web hosting appliances allows any local user the ability to modify the FrontPage site.	Patch available at: RaQ3i (Intel x86): ftp://ftp.cobaltnet.com/pub/experimental/security/frontpage/fpx_patch1.tar.gz RaQ2 (MIPS): ftp://ftp.cobaltnet.com/pub/experimental/security/frontpage/fpx_patch1.tar.gz	Cobalt FrontPage Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Danware[6] Windows 3x/95/98/ NT 4.0/2000	NetOp 6.0. 6.50	The file transfer mechanism requires no authentication, which could give a remote malicious user full read/write access to the system's file system.	NetOp version 6.50 has the ability to use either NetOp or Windows security to authenticate users immediately upon connection, although this is not enabled by default.	NetOp Remote Control Unauthent-icated File Transfer	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Deerfield Communi-cations[7] Windows 95/98/NT 4.0/2000	Mdaemon 3.0.3	A denial of service condition exists if greater than 256 characters are passed to the username on login.	Patch available at: ftp://ftp.altn.com/Mdaemon/Release/	Mdaemon Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Ecommerce Exchange[8]	Quick Commerce	A vulnerability exists that allows a malicious user the ability to download a form purchase page and alter the contents to obtain free products.	No patch or workaround available at time of publishing.	Quick Commerce Insecure Transaction Process	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Bugtraq, May 25, 2000.
[4] Solar Designer, May 30, 2000.
[5] Chris Adams, May 23, 2000.
[6] b0f-SA2000-002, April 12, 2000.
[7] Bugtraq, May 24, 2000.
[8] 14x Network Security Inc., May 22, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[9] Unix	FreeBSD 3.x and below Libmytinfo	A buffer overflow exists against libmytinfo that will allow a malicious user the ability to execute arbitrary code on the system.	Upgrade to FreeBSD 4.0 or follow unofficial workaround at: http://www.securiteam.com/unixfocus/Buffer_overflow_in_libmytinfo_elevates_local_user_s_privileges.html	FreeBSD Libmytinfo Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[10]	Hewlett-Packard Web JetAdmin Version 5.6	A vulnerability exists with the HP Web JetAdmin 5.6 Web interface Server on port 8000 that allows a malicious user read access to any file on the web-published filesystem.	Upgrading to Version 6.0 will eliminate this vulnerability. http://www.hp.com/cposupport/swindexes/hpwebjetad1880_swen.html	HP Web JetAdmin Directory Traversal Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Hewlett-Packard[11]	Hewlett-Packard Web JetAdmin Version 6.0	A denial of service condition results if a malicious user sends malformed URL requests to port 8000, which will cause the process to stop responding.	No patch or workaround available at time of publishing.	HP Web JetAdmin Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
IBM[12]	Lotus Domino	Web pages can be edited remotely if permissions are not set properly and design conditions are not taken into account.	Workaround published at: http://www.securiteam.com/exploits/Lotus_Domino_Server_allows_documents_to_be_modified_remotely.html	Domino Remote Document Modification	Low	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[13]	Lotus Domino 5.0.1	A denial of service exists if a remote malicious user sends a buffer overflow to the SMTP service. The service will crash and potentially make it possible to execute arbitrary commands on the system.	No patch or workaround available at time of publishing.	Domino Remote SMTP Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ITHouse[14] Windows 3.51/95/NT 4.0	ITHouse Mail Server 1.0.4	A buffer overflow vulnerability exists which could allow a remote malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	ITHouse Mail Server 1.04 Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[9] SecuriTeam, May 19, 2000.
[10] USSR Labs, May 24, 2000.
[11] USSR Labs, May 24, 2000.
[12] SecuriTeam, May 27, 2000.
[13] SecuriTeam, May 27, 2000.
[14] Delphis Consulting Plc Security Team Advisories, DST2K0007, May 30, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
KDE[15] **Unix** ***SuSE has released updated packages.***[16]	**KDE 1.1, 1.1.1, 1.2, 2.0 BETA**	**A vulnerability exists which allows the SHELL variable to be altered to execute something other than the shell. This lets a local malicious user gain UID disk, which can then be used to gain root.**	**No workaround or patch available at time of publishing.** ***Updated package available at:*** ftp://ftp.suse/com/pub/suse	**KDE Kscd SHELL Environmental Variable**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Mandrake-Soft[17] Unix	Mandrake 7.02 Kdesud	A buffer overflow exists in kdesud that will allow a malicious user to gain root privileges on the system.	Patch available at: http://www.linux-mandrake.com/en/fupdates.php3	Mandrake Kdesud Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mandrake-Soft[18] Unix	Mandrake 7.0	A buffer overflow vulnerability exists in the cdrecorder binary, which could let a malicious user execute arbitrary commands. Other distributions of Linux may be vulnerable to this problem as well.	No workaround or patch available at time of publishing.	Linux cdrecord Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Martin K. Peterson[19] Unix	gdm 2.0.x BETA + GNOME, GNOME 1.0.x, gdm 1.0.x + GNOME, GNOME 1.0.x	A buffer overflow vulnerability exists in the XDMCP handling code used in 'gdm', which could allow a remote malicious user the ability to execute arbitrary commands as root.	SuSE has released updated packages available at: ftp://ftp.suse.com/pub/suse TurboLinux has released updated packages available at: ftp://ftp.turbolinux.com/pub/updates/6.0/security	GNOME gdm XDMCP Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
McMurtrey/ Whitaker & Associates, Inc.[20]	Cart32 (Verified in versions 2.5a and 3.0)	A vulnerability exists that allows a malicious user to download and alter the purchase form to buy products at a desired price.	No patch or workaround available at time of publishing.	Cart32 Insecure Transaction Process	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
MetaProducts[21] Windows 95/98/NT 4.0/2000	Offline Explorer 1.1	A vulnerability exists that allows a malicious user the ability access files on the remote system using the "GET ..\.." command. In addition, Offline Explorer starts a server on port 800, through which the downloaded web pages can be viewed.	No workaround or patch available at time of publishing.	Offline Explorer Directory Traversal Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[15] Bugtraq, May 17, 2000.
[16] SuSE Security Announcement, May 29, 2000.
[17] Bugtraq, May 26, 2000.
[18] Bugtraq, May 27, 2000.
[19] Bugtraq, May 22, 2000.
[20] bunny69, May 22, 2000.
[21] Bugtraq, May 22, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[22] Windows NT 4.0	SQL Server 7.0 Service Pack 1.0, 2.0, SQL Server 7.0	A security vulnerability exists in the installation routine of Service Packs 1 and 2. When run on a machine that is configured in a non-recommended mode, the routines record the administrator password in a log file, where it could be read by any user who could log onto the server at the keyboard.	Microsoft has released a patch for Service Pack 2, which rectifies this issue. For those running Service Pack 1, search for SQLSP.LOG and delete it. If Service Pack 1 is reinstalled, be sure to delete SQLSP.LOG again and if Service Pack 2 is redeployed, apply the patch again. Microsoft SQL Server 7.0: http://download.microsoft.com/download/sql70/SPpwfix/7.0/WIN98/EN-US/SQLSP.exe For those running Service Pack 2. Be sure to extract this file to either X86\Setup or Alpha\Setup, depending on the processor architecture of the server	SQL Service Pack Password	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[23] Windows 95/98/NT 4.0/2000	Windows 95/98 NT 4.0 Workstation, Server, Server Enterprise Edition, Server, Terminal Server Edition, 2000 Professional, Server, Advanced Server	A denial of service vulnerability exists when large numbers of identical fragmented packets are sent, which causes the target machine to lock-up for the duration of the attack.	Patch available at: Windows 95: http://download.microsoft.com/download/win95/update/8070/w95/EN-US/259728USA5.exe Windows 98: http://download.microsoft.com/download/win98/update/8070/w98/EN-US/259728USA8.exe Windows NT 4.0 Workstation, Server, Server Enterprise Edition: http://www.microsoft/com/Downloads/Release.asp?ReleaseID=20829 Windows NT 4.0 Server, Terminal Server Edition: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20830 Windows 2000 Professional, Server and Advanced Server: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20827	IP Fragment Reassembly CVE name CAN-2000-0305	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[22] Microsoft Security Bulletin, MS00-035, May 30, 2000.
[23] Microsoft Security Bulletin, MS00-029, May 19, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[24] Windows 95/98/ NT 4.0/2000	Windows 95/98/ NT 4.0/2000 Windows NT Terminal Server	Because of the inability of administrators to limit whether Master Browsers respond to certain frames, two vulnerabilities exist. They are: 1.) the Reset Browser Frame vulnerability, whereby there is no capability to configure a browser to ignore ResetBrowser frames, which could allow a malicious user to shut down browsers on his subnet or declare his machine the new Master Browser; and 2.) the HostAnnouncement Flooding vulnerability, which could allow a malicious user the ability to send a huge number of bogus HostAnnouncement frames to a Master Browser.	Patch available at: Microsoft Windows NT 4.0: http://download.microsoft.com/download/winntsp/Patch/Q262694/NT4ALPHA/EN-US/Q262694a.EXE Alpha: http://download.microsoft.com/download/winntsp/Patch/Q262694/NT4ALPHA/EN-US/Q262694i.EXE Microsoft Windows NT 2000: Http://download.microsoft.com/download/win2000platform/Patch/Q262694/NT5/EN-US/Q262694_W2K_SP2_x86_en.EXE	ResetBrowser Frame and Host Announcement Flooding	Low	Bug discussed in newsgroups and websites.
Microsoft[25] Windows 95/98/NT	Windows Media Encoder 4.0-4.1	A vulnerability exists in which a request with a particular malformation sent to an affected encoder would cause the encoder to fail, thereby denying formatted content to the Windows Media Player.	Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21596	Malformed Windows Media Encoder Request	Low	Bug discussed in newsgroups and websites.
Microsoft[26] Windows NT 2000	Windows NT 2000	A security vulnerability exists which could make it easier for a malicious user who had complete control over a Windows 2000 machine to compromise users' sensitive information.	Patch available at: http://download.microsoft.com/download/win2000platform/Update/Q260219/NT5/EN-US/Q260219_W2K_SP1_x86_en.EXE	Microsoft Windows 2000 Protected Store Key Length	**High**	Bug discussed in newsgroups and websites.
Multiple Systems[27]	Majordomo 1.94.5	A vulnerability exists in some of the Perl programs that allow a local user to force majordomo to execute arbitrary commands on the system.	Red Hat packages available at: ftp://ftp.redhat.com/redhat/updates/powertools/6.1/i386/majordomo-1.94.5-2.i386.rpm Unofficial workaround discussed at: http://www.securiteam.com/exploits/Additional_majordomo_security_vulnerabilities.html	Majordomo Insecure Implementation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[24] Microsoft Security Bulletin, MS00-036, May 26, 2000.
[25] Microsoft Security Bulletin, MS00-038, May 31, 2000.
[26] Microsoft Security Bulletin, MS00-032, June 2, 2000.
[27] Federico Schwindt, May 23, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[28] ***New exploit scripts have been published.***[29]	**Cygnus Network Security 4.0.x, KerbNet 5.0.x; MIT Kerberos 4 4.0 patch 10, 5 5.0-1.1.1, 5 5.0-1.0.x**	**Several buffer overrun vulnerabilities exist which could allow a remote malicious user to gain root access.**	**Patches are available against krb5-1.0.x., and krb5-1.1.1 MIT Kerberos 5 5.0-1.1.1: http://www.securityfocus.com/data/vulnerabilities/patches/krb5-1.1.1.patch MIT Kerberos 5 5.0-1.0.x: http://www.securityfocus.com/data/vulnerabilities/patches/krb5-1.0.x.patch MIT will release krb5-1.2 shortly, which will remedy these problems in the MIT codebase.**	**Kerberos Compatibility krb_rd_req() Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.** ***Two exploit scripts have been published.***
Multiple Vendors[30] Unix	SuSE Linux 4.0-4.4.1, 5.0-5.3, 6.0-6.4, 7.0; Slackware Linux 3.3, 3.4, 3.5, 3.6, 3.9, OpenLinux 7.0; TurboLinux Turbo Linux 6.0-6.0.2	A buffer overflow vulnerability exists in the 0.8 version of the fdmount program, distributed with a number of popular versions of Linux, which could allow a malicious user in the 'floppy' group the ability to execute arbitrary commands as root.	A patched fdmount which replaces the offending sprintf() call with a vsnprintf() has been posted in an updated floppy.tgz package in Slackware-current. Please download the new floppy.tgz and run upgradepkg on it. ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/a1/floppy.tgz Temporary workaround: Remove the setuid bit on the fdmount binary, or remove non-trusted users from the 'floppy' group.	Multiple Linux Vendor fdmount Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Multiple Vendors[31] Unix	Xlockmore 4.16 and below	An implementation vulnerability exists in xlock that allows global variables in the -mode argument initialized section of memory to be overwritten. This would allow the user to read the passwd file.	Patch available at: ftp://ftp.tux.org/pub/tux/bagleyd/xlockmore/index.html Select either xlockmore-4.16.1.tar.gz or xlockmore-4.16-4.16.1.diff.gz	Multiple Vendor Xlockmore Memory Reading Vulnerability	**High**	Bug discussed in newsgroups and websites.

[28] ANSIR Advisory, May 19, 2000.
[29] Bugtraq, May 18, 2000.
[30] Bugtraq, May 22, 2000.
[31] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-06, May 29, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[32, 33] Unix	FreeBSD 5.0, 5.0 alpha, FreeBSD 4.0, 4.0 alpha, FreeBSD 3.x, 2.2.8,2.2.2-2.2.6, 2.2, 2.1.7.1, 2.1.6.1, 2.1.6, 2.1.5, 2.1, 2.0.5, 2.0, 1.1.5.1; All NetBSD prior to 2000/05/27; OpenBSD 2.6, 2.5, 2.4, 2.3, 2.2, 2.1, 2.0	An undocumented kernel semaphore control call can be used by a malicious user to cause all processes waiting on semaphores to block, resulting in a denial of service of all applications using semaphores.	**FreeBSD:** Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:19/semconfig.patch **OpenBSD:** A patch is available at Http://www.openbsd.org/errata26.html#semconfig **NetBSD:** For NetBSD 1.4, 1.4.1, and 1.4.2: a patch is available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/20000527-sysvsem For NetBSD-current: NetBSD-current since 20000527 contains all the fixes, and is not vulnerable. Users of NetBSD-current should upgrade to a source tree dated 20000527 or later.	Multiple Vendor BSD Semaphore IPC Denial Of Service	Low	Bug discussed in newsgroups and websites.
NetBSD[34] Unix	NetBSD 1.4.2 Ftpchroot	A vulnerability exists that allows users listed in /etc/ftpchroot access to files outside their home directory.	Patch available at: ftp://ftp.netbsd.org/pub/NetBSD/misc/security/patches/20000527-ftpd	NetBSD ftpchroot Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[35]	Netscape 4.73 and below without Personal Security Manager	A vulnerability exists that could allow a malicious user the ability to masquerade as a legitimate web site if that user can compromise certain DNS information.	Install Personal Security Manager. CERT workaround and discussion available at: http://www.cert.org/advisories/CA-2000-08.html	Netscape Inconsistent Warning Messages	Medium	Bug discussed in newsgroups and websites.
Network Associates Inc.[36] Unix	Gauntlet 4.1, 4.2, 5.0, and 5.5 running Webshield CyberPatrol daemon; WebShield 100 series E-ppliance, WebShield 300 series E-ppliance, WebShield For Solaris 4.0	A buffer overflow exists within the WebShield CyberDaemon and cause a denial of service to the HTTP service, thus disallowing any Web traffic. In addition, the buffer overflow may be exploited to execute arbitrary code on the system.	All versions except Gauntlet 4.1 can be patched: www.pgp.com/jump/gauntlet_advisory.asp#patches Official workaround for 4.1 is at: http://www.securiteam.com/securitynews/Gauntlet_Firewall_for_Unix_and_WebShield_CyberDaemon_buffer_overflow_vulnerability.html	Gauntlet and Webshield CyberPatrol Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press.

[32] FreeBSD Security Advisory, FreeBSD-SA-00:19, May 30, 2000.
[33] NetBSD Security Advisory, 2000-004, May 27, 2000.
[34] NetBSD Security Advisory, 2000-006, May 28, 2000.
[35] CERT, May 26, 2000.
[36] SecurityFocus, May 22, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Network Associates Inc.[37] Windows NT	Gauntlet for NT 5.0 (unpatched, and with hotfixes 1,2,3) Gauntlet for NT 5.5 (unpatched, and with SP1 and hotfixes 1,2,3,4)	A vulnerability exists in which the firewall performs Network Address Translation (NAT) in an unexpected manner, causing incorrect routable IP addresses to be generated. This can enable unprivileged users on the protected network to generate spurious source IP addresses. In addition, this could lead to a denial of service to targeted address spaces.	No patch or workaround available at time of publishing.	Gauntlet NAT Mishandling	Medium	Bug discussed in newsgroups and websites.
Network Associates Inc.[38] Unix	PGP 5.0	A vulnerability exists that will allow, under certain circumstances, the generation of insecure public/private key pairs.	Vendor recommends upgrade to version 6.5 and discontinue use of insecure public/private key pairs.	PGP Insecure Key Generation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Network Associates, Inc.[39] Windows NT 4.0 Server	Webshield SMTP 4.5.44 Management Tool	The Management Tool on port 9999 within Webshield allows a connection that permits a malicious user read and write access to the configuration files.	No patch or workaround available at time of publishing.	Webshield Configuration Modification Vulnerability	Medium	Bug discussed in newsgroups and websites.
PDGSoft[40] Windows NT/Unix	PDGSoft Shopping Cart	Two buffer overflows in two separate executables associated with the PDGSoft Shopping Cart allow a remote malicious user the ability to execute arbitrary code.	Patch available at: http://www.pdgsoft.com/Security/security2.html	PDGSoft Remote Buffer Overflow vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm[41] Unix	Qpopper 2.53	A vulnerability exists which could allow a malicious user the ability to execute arbitrary code. Requires an account on the machine.	Upgrading to versions 3.0.1 or later located at; Qualcomm qpopper 2.53: http://www.eudora.com/qpopper/#CURRENT Qualcomm qpopper 2.52: http://www.eudora.com/qpopper/#CURRENT	Qpopper Remote Shell Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Rockliffe[42] Windows NT	MailSite-HTTPMA/4.2.1.0	A buffer overflow exists in the Rockliffe MailSite Management Agent that allows a remote malicious user the ability to execute arbitrary code.	Upgrade to patched version 4.2.2 http://www.rockliffe.com/	MailSite Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[37] SecuriTeam, May 27, 2000.
[38] ISN, May 23, 2000.
[39] Delphis Consulting Plc, May 5, 2000.
[40] Cerberus, May 25, 2000.
[41] buffer0verfl0w Security Advisory, b0f-SA2000-005, May 23, 2000.
[42] Cerberus Information Security Advisory, CISADV000524a, May 24, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SGI[43] Unix	IRIX 6.5-6.5.7 Infosearch	A vulnerability exists in the infosrch.cgi program that gives a remote malicious user the ability to view files on the system with the privileges of the user "nobody."	Patch available at: http://www.sgi.com/Support/security/	IRIX Infosearch Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE[44] Unix	SuSE 6.1-6.4 Kernel 2.2.15	A vulnerability exists in the masquerading feature of the Linux kernel that allows arbitrary backward connections to be opened and could cause a denial of service.	Patch available at: ftp://ftp.suse.com/pub/suse/i386/update/6.4/	SuSE Kernel Denial of Service	Low	Bug discussed in newsgroups and websites.
SuSE[45] Unix	SuSE 6.1-6.4 Kmulti 1.1.2	A vulnerability exists that permits local users the ability to execute commands as root.	Patch available at: ftp://ftp.suse.com/pub/suse/i386/update/6.1/kde1/kmulti-1.1.2-141.i386.rpm	SuSE Kmulti Root Compromise	**High**	Bug discussed in newsgroups and websites.
Symantec[46]	PcAnywhere versions 7.5 to 9.2	PcAnywhere configuration files are vulnerable to weak password encryption.	Vendor suggests turning on public key encryption.	PcAnywhere Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Xfree[47] Unix	Xfree96 3.3.5, 3.3.6, 4.0	A vulnerability exists that will cause the victim X server to freeze and lock the keyboard and potentially the mouse.	The upgrade packages can be found at: Ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/ The corresponding source code package can be found at: Ftp://ftp.calderaystems.com/pub/updates/OpenLinux/2.3/current/SRPMS	Multiple Vendor Xfree86 Malformed Packet Freeze	Low	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[43] SGI Security Advisory, May 22, 2000.
[44] SuSE Security, May 18, 2000.
[45] SuSE Security, May 29, 2000.
[46] SecuriTeam, May 19, 2000.
[47] Caldera Systems, Inc. Security Advisory, CSSA-2000-012.0, May 18, 2000.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 18 and June 1, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 73 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 1, 2000	Funkysh lsi_v1.0_RH.sh	TSS v1.0beta1 is a shell script to check the local security of a Red Hat 6.0 / 6.1 / 6.2 machine.
June 1, 2000	Kill_sntsd.pl	Remote buffer overflow in Simple Network Time Sync daemon and client version 1.0, tested on Redhat 6.1.
June 1, 2000	Mail_bof.c	/usr/bin/Mail local Linux exploit which gives gid=12 shell. Tested against Slackware 3.6 and 7.0.
June 1, 2000	Mailx.c	Mailx local exploit - Tested on Slackware 3.6, 4.0, and 7.0 and Debian 2.0r2, 2.1, 2.2.
June 1, 2000	Major2.c	Exploit script for Majordomo Insecure Implementation Vulnerability.
June 1, 2000	Retina.exe	Remote network mapping and vulnerability scanner package with artificial intelligence features that allow it to think like a hacker and find unknown vulnerabilities using Common Hacking Attack Methods (CHAM).
May 31, 2000	b0g-5.txt	B0g Issue 5: RFP interview, credit card algorithms, GNOME coding, Nokia cell phone information, and ICQ information.
May 31, 2000	Magdalena.pl	A small utility written in Perl that will scan a list of hostnames for a certain CGI.
May 31, 2000	Majordomo.txt	Discussion and exploit script for Majordomo vulnerabilities.
May 31, 2000	Msbddos.c	Exploit script for the Malformed Windows Media Encoder Request vulnerability.
May 30, 2000	Ecrack-0.1.tgz	ECrack v0.1 –IRC (bot) brute force password cracker.
May 30, 2000	Execve-shell.tar.gz	Create Linux x86 shellcode that executes any command.
May 30, 2000	Hunt-1.5.tgz	A program for intruding into a TCP connection.
May 30, 2000	Icq.web.front.dos.txt	CQ Web Front Remote denial of service vulnerability - ICQ 2000a, 99b, and 99a contain a vulnerability in the personal web server.
May 30, 2000	Kdesud-xpl.c	Exploit script for Mandrake kdesud Buffer Overflow.
May 30, 2000	Shadyshell.c	Lightweight, UDP portshell.
May 30, 2000	Snuff-v0.8.1.tar.gz	Multi-stream packet sniffer for Linux 2.0/2.2.
May 30, 2000	Swstack.txt	Advisory for Simple Web Server 0.5.1 buffer overflow.
May 30, 2000	Wemilo.tcl	Remote Cart32 exploit.
May 28, 2000	5niffi7.c	Remote root exploit for sniffit (-L mail) 0.3.7.beta on Debian 2.2.
May 28, 2000	Elm-ex.c	Elm 2.5 PL3 exploit tested under Linux Slackware 3.6, 4.0, 7.0.
May 28, 2000	Nmap-2.54BETA1.tgz	Nmap v2.54.
May 28, 2000	Sniffit_NT.0.3.7.beta.zip	Sniffit 0.3.7 beta for Windows NT/2000.
May 27, 2000	Animal.c	Exploit script for Gauntlet and Webshield CyberPatrol Buffer Overflow.
May 27, 2000	Breakgdm.c	Exploit script for SuSE gdm Buffer Overflow vulnerability.
May 27, 2000	**Cdburner-exp.c**	**Exploit script to get gid-80 group cdwriter via /usr/bin/cdrecord vulnerability.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 27, 2000	Fd-ex.c	Exploit script for the Multiple Linux Vendor fdmount Buffer Overflow vulnerability.
May 27, 2000	Fdmnt-smash.c	Exploit script for Slackware Fdmount Buffer OverFlow for Slackware version 4.0.
May 27, 2000	Fdmnt-smash2.c	Exploit script for Slackware Fdmount Buffer OverFlow for Slackware version 7.0.
May 27, 2000	Fdmount_xplt.c	Exploit script for the Multiple Linux Vendor fdmount Buffer Overflow vulnerability.
May 25, 2000	Arpci2.1.21.tar.gz	RPCI2 automates the task of sending rpcinfo requests to a mass of hostnames.
May 25, 2000	Arpgen.tar.gz	A denial of service tool which demonstrates a flood of ARP requests from a spoofed Ethernet and IP address.
May 25, 2000	Obsd_ipfhack.c	LKM for OpenBSD which makes ipfilter always accept packets from a certain IP.
May 25, 2000	Xsh0k.c	Xwindows remote DoS attack.
May 24, 2000	Ciscowebdos.pl	Cisco IOS Router DoS.
May 24, 2000	Labs41.txt	USSR Advisory #41 - HP Web JetAdmin web interface server directory traversal vulnerability.
May 24, 2000	Labs42.txt	USSR Advisory #42 - HP Web JetAdmin remote denial of service attack.
May 24, 2000	Mdbms.c	Exploit script for MDBMS 0.96b6 vulnerability.
May 24, 2000	Pat2.tgz	Ping Analysis Tool II.
May 24, 2000	Saint-2.1.beta2.tar.gz	SAINT 2.1 Beta 2.
May 24, 2000	Sara-3.0.5.tar.gz	SARA 3.0.5.
May 24, 2000	Scs11.zip	Simpsons CGI Scanner v1.1.
May 23, 2000	B0f5-Qpopper.txt	Exploit script for the Remote Shell via Qpopper 2.53 vulnerability.
May 23, 2000	CiscoAuditingTool-v1.tar.gz	Perl script which scans Cisco routers for common vulnerabilities.
May 23, 2000	Cisconuke.c	Script which reboots Cisco routers.
May 23, 2000	Induce-arp.tg	Remote OS detection program which uses SRP fingerprinting.
May 23, 2000	Killsentry.c	Script that shows that automatic firewalling is a bad idea by sending spoofed FIN packets from different hosts in an attempt to confuse Portsentry.
May 23, 2000	Qpop_euidl.c	Exploit script for the Qpopper vulnerability.
May 23, 2000	**Smtpkill.pl**	**Script which exploits the Lotus Domino ESMTP vulnerability.**
May 23, 2000	Sniffitexp.c	Sniffit 0.3.7Beta remote exploit script which runs on RedHat 6.0.
May 23, 2000	Socket-dos.c	SSH 1.2.27 exploit script that creates a Unix domain socket with an arbitrary file names anywhere in the file system.
May 22, 2000	Infosh.pl	Exploit script for the IRIX Infosrch.cgi vulnerability.
May 20-22, 2000	Dsniff-2.1.tar.gz	Suite of utilities that is used for penetration testing.
May 20-22, 2000	Joe-fixed.c	Proof-of-concept script for the Joe v2.8 stack overflow vulnerability.
May 20-22, 2000	Kshux.c	Remote root exploit for the kerberos vulnerability.
May 20-22, 2000	Ksux.c	Remote root exploit for the kerberos vulnerability.
May 20-22, 2000	Nscan0666b10ff.zip	Portscanner, which scans up to 200 ports per second, for networks with smart whois, traceroute, host lists for rescanning and numerous other features.
May 20-22, 2000	Nslookupsploit.c	Nslookup exploit script for Linux.
May 20-22, 2000	Pirchslap.exe	Pirch98 IRC client Denial of Service.
May 20-22, 2000	Portscanner010.zip	Port scanner written in Java 1.3.
May 20-22, 2000	Shellhit.c	Buffer overflow exploit script for TESO Hellkit.
May 20-22, 2000	Sock.c	Script which enables all users to open raw sockets.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 20-22, 2000	Sscan2k-pre2.b0f.tar.gz	Sscan2k now has updated vulnerability checks along with an improved OS detection.
May 20-22, 2000	Ucgi240.c	CGI vulnerability scanner which checks for 407 CGI vulnerabilities.
May 19, 2000	Cproxy.c	Remote DoS script for Cproxy 3.3.
May 19, 2000	Jolt2.c	Exploit script for Windows IP Fragmented Packet Denial of Service.
May 19, 2000	Klogin.c	Exploit script for the BSDI klogin root buffer overflow vulnerability.
May 19, 2000	**Pcax.c**	**Exploit script for PcAnywhere Weak Password Encryption vulnerability.**
May 19, 2000	Xsol.c	Local root exploit script for the xsoldier vulnerability.
May 18, 2000	10pht10-he-kid.c	Easy antisniff 1.02 exploit script.
May 18, 2000	10pht10phc.c	Easy antisniff 1.02 exploit script.
May 18, 2000	ADMDNews.zip	Windows NT/Win2K x86 exploit script for the NetWin Dnews server vulnerability.
May 18, 2000	Arpmitm-0.1.tar.gz	Tool or using ARP man-in-the-middle attacks.
May 18, 2000	Gnomelib.sh	SuSE 6.3 and Gnomelib local root exploit script.
May 18, 2000	Sniffit.c	Sniffit 0.37beta remote exploit script.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

- An increasing number of reports of intruders using nameservers to execute packet-flooding Denial of Service attack.
- Reports of a combination of tools called "mstream." The purpose of the tool is to enable intruders to utilize multiple Internet connected systems to launch packet-flooding Denial of Service attacks against one or more target systems. A tool that allows users to identify the presence of mstream on host systems can be found on the NIPC website at http://www.nipc.gov/advis00-044.htm.

Probes/Scans:

- An increase in scans for Klogin ports (Kerberos vulnerabilities).
- An increase in scans from China.
- An increase in scans to port 109 (pop2 exploit).
- There has been an increase in probes to UDP Port 137 (NetBIOS Name Service).
- There has been additional discussion concerning the AMDROCKS BIND exploit.

- An increase from Brazil in exploits and scans to port 53 are being used against well-known vulnerabilities: the NXT overflow vulnerability, which creates the directory ADMROCKS after entry; and the BIND vulnerability.
- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at ports 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

Other:

- **Additional variants of the "I Love You" virus continue to emerge and are becoming increasingly destructive.**
- **Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running).**
- **An increase in amd exploits.**
- Reports indicate that there is increasing interest in the Trojan capabilities of Gnutella, a free filesharing utility similar to Napster.
- Certain virus e-mail gateways are reportedly not catching all virus signatures.
- An increase in reports of intruders exploiting unprotected Windows networking shares.
- An increase in exploitation of unprotected Windows networking shares.
- Reports indicate registry objects being maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

O97M/Cybernet.A (Microsoft Office 97 Macro Virus): This virus has been reported in the wild and is a Melissa-like virus with worm-like capabilities. The virus primarily infects Word and Excel 97, and uses the first 50 e-mail addresses within the user's address book.

The virus will come as an e-mail with the subject "You've GOT Mail !!!" and the following message:

> "Please, saved the document after you read and don't show to anyone else. The document is also VIRUS FREE…so DISREGARD the virus protection warning !!!"

The virus has embedded code to avoid detection. Anti-virus researchers have found the following comments:

> "anti-heuristic for stupid Norton antivirus scanner"
> "anti-heuristic for stupid McAfee antivirus scanner"

There are two payloads, which will trigger on 17th August and 25th December.

The virus will insert into any currently open Word or Excel document a series of random shapes. This aspect is similar to WM97/Melissa-AG. The virus will insert into the AUTOEXEC.BAT the command to format the C: drive of Windows 98 systems and will also modify the CONFIG.SYS. Finally, the virus will display a message box and once the "OK" button that is displayed is Pressed, the machine will restart and execute the commands above.

VBS/CoolNote (Visual Basic Script Worm): The worm arrives in an e-mail with the subject "Cool Notepad Demo" and contains the text "Hey check out this text file I sent it will do something neat in notepad Enjoy :-)". The virus is contained in the attachment "COOL_NOTEPAD_DEMO.TXT.vbs". If executed, the virus will modify the c:/mirc/script.ini file if present. If the virus detects the presence of mIRC, it will copy itself into the Windows System folder. The virus will make changes to the Registry that disables the desktop.

VBS/Fireburn.worm (Visual Basic Script Worm): This is a Visual Basic Script worm that spreads via Outlook and mIRC and is a variant of the **VBS/LoveLetter-A.** When the worm is run, it saves a copy of itself in c:\windows\rundll32.vbs, and alters the Registry so that this program is run on startup. The script looks for a mIRC client in either c:\MIRC or c:\Program Files\mirc. If the client is found, the worm overwrites the script.ini file with a new file so as to send itself to people on the channel.

The worm checks for the existence of "C:\Programme" and will then e-mail copies of itself in German to all entries in the Outlook address book. If "C:\Programme" does not exist, the e-mails will be in English. The German e-mails will have the subject "Moin, alles klar?" and have the text "Hi, wie geht's dir? Guck dir mal das Photo im anhang an, ist echt geil ;) bye, bis dann." The English e-mails will have the subject "Hi, how are you?" and contain the text in the body "Hi, look at that nice Pic attached ! Watching it is a must ;) cu later…".

A .vbs attachment will arrive. A copy of the worm with the same name that was contained in the attachment will be created in the Windows directory. The worm will rename Rundll32.vbs to suggest it contains a pornographic picture and attaches to each e-mail. The worm will delete these e-mails from the sent folder to avoid detection.

If the date is June 20, the worm displays a message box containing the txt "I'm proud to say that you are infected by FireburN!" The worm will change the "Registered Owner" field in MyComputer/Properties" to the new value "FireburN" via modifying the registry key.

W32/NewApt-A (Worm): This is a variant of W32/Newapt and propogates through e-mail as an attachment. The file will have one of 25 different names chosen randomly from an internal list. If the attachment is run, the worm will display a dialog box. The worm will concurrently search the hard drive for Outlook E-mail addresses. The worm has a trigger date of December 26th, whereby the worm will attempt to connect to any Microsoft brand equipment every 3 seconds.

W32/NewApt-C (Worm): This variant of W32/NewApt has the same attributes as **W32/NewApt-A** with the exception of the trigger date of February 2, whereby the worm will attempt to connect to any Microsoft brand equipment every 3 seconds.

WM97/Akuma-D (Word 97 Macro Virus): This virus has been reported in the wild. The virus is complex, and will select a random day within a 30-day period of infection. It will then display a message box with one of these titles: The World; Killer Queen; Vanilla Ice; Star Platinum; Crazy Diamond; or Dr. Watson, and will then attempt to delete all files on the C:, D:, and E: drives.

WM97/Bobo-C (Word 97 Macro Virus): A simple Word 97 Macro Virus that has no payload.

WM97/Ciao-A (Word 97 Macro Virus): The virus will occasionally insert text into infected Word documents. When a new document is created, the virus inserts the French text "Microsoft vous souhait" if a complex date trigger is activated. When the document is closed, the virus inserts "Ciao!!!" into the document. If another complex date trigger is activated, the virus will display a message box.

WM97/Heathen (Word 97 Macro Virus): This is a Word 97 macro virus that will infect the global template. WM97/Heathen will disable Word macro antivirus protection. It will also use several support files within Windows 95 for the purpose of infecting the global template. The virus' payload will trigger 6 months from the date of first infection. The virus will delete all files within the Windows Registry (primarily the USER.DAT and SYSTEM.DAT files and their backups, USER.DA0 and SYSTEM.DA0). This will cause subsequent reboots of Windows to fail, and force a reinstallation.

WM97/IIS-U (Word 97 Macro Virus): This virus has been reported in the wild. WM97/IIS-U is a polymorphic macro virus that uses randomly created variable names and inserts randomly created instructions into the virus code for additional virus generations. The virus can generate corrupted samples of itself, due to faults within the random variable names generator routine.

WM97/Marker-AO (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Marker Word 97 Macro Virus. This virus is similar to the above WM97/Marker-DJ variant.

WM97/Marker-DJ (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Marker Word 97 Macro Virus. The virus will take information in the File/Properties/Summary menu whenever a document is closed. The virus will then FTP the information to the Codebreakers website. The virus will also attach the sender's user information to the bottom of the macro as a comment.

WM97/Melissa.BG (Word 97 Macro Virus and E-mail Worm – popularly called the "Resume" virus): This is another variant of the WM97/Melissa virus. This new variant deletes files on local and shared drives when an infected document is closed. It attempts to spread to everyone in available address books and tries to delete all files in the following directories and drives. The infected file attachment has an e-mail subject of "Resume-Janet Simons" with attachment "Explorer.doc." The worm tries to delete all files in the following directories and drives:

C:*.*
C:\My Documents*.*
C:\WINDOWS*.*
C:\WINDOWS\SYSTEM*.*
C:\WINNT*.*
C:\WINNT\SYSTEM32*.*
A:*.* [may cause an error message]
B:*.* [may cause an error message]
and *.* in the root of drives D: thru Z:

The e-mail will arrive with the following format: Subject: Resume - Janet Simons. The body of the e-mail reads:

> To: Director of Sales/Marketing,
>
> Attached is my resume with a list of references contained within. Please feel free to call or e-mail me if you have any further questions regarding my experience.
>
> I am looking forward to hearing from you.
>
> Sincerely,
> Janet Simons.

There will be an attached file named "Explorer.doc".

This worm attempts to delete files on your hard drive, mapped network drives, floppy disks and zip drives. *If you receive an e-mail that matches this description, please delete it immediately.* The correct action is to ensure no one opens the attachment and, even better, to set up e-mail filters that stop any offending messages. Tell people to deactivate their executive summary feature in Microsoft Outlook, and only then delete the e-mail without opening.

Valuable data from the top virus vendors (those involved in maintaining the Information Security DEW Line [Digital Early Warning Line]) can be found at:

- Norton Anti Virus: http://vil.nai.com/villib/dispvirus.asp?virus_k=98661
- Symantec: http://www.symantec.com/avcenter/venc/data/w97m.melissa.bg.html

WM97/Smac-E (Word 97 Macro Virus): This virus has been reported in the wild. This virus will only work on double-byte language versions of Word. The United States primarily uses a single-byte language version. There are two potential payloads. The first will attempt to open a million message boxes containing non-Roman characters on September 2. The second payload will open a message box displaying non-Roman characters on the 13th of each month.

WM97/Thursday-Z (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Thursday virus. On December 13th, the virus attempts to delete all files and subdirectories on your computer's C: drive.

XM97/Barisada-A (Excel 97 Macro Virus): This virus has been reported in the wild. The virus macros are stored in the file HJB.XLS. On 24 of April each year between 2pm and 3pm, the virus displays a series of questions related to a role-playing game. The first dialog box has the title "1st Qusetion" [sic] and the text "Question : What is the Sword Which Karl Syner (=Grey Scavenger) used? Arswer: Barisda."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
AOL Trojan		CyberNotes-2000-01
Asylum	v0.1	CyberNotes-2000-10
AttackFTP		CyberNotes-2000-10
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92	CyberNotes-2000-09
Bla	1.0-5.02	CyberNotes-2000-06
Bla	v1.0 - 5.03	CyberNotes-2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
Drat	v1.0 - 3.0b	CyberNotes-2000-09
FakeFTP	Beta	CyberNotes-2000-02
GIP		**Current Issue**
Girlfriend	v1.3x (including Patch 1 & 2)	CyberNotes-2000-05
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hack`a`Tack	1.2-2000	CyberNotes-2000-06
Hack'A'tack	1.0-2000	CyberNotes-2000-01
ICQ PWS		**Current Issue**
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4	CyberNotes-2000-01

Trojan	Version	Issue discussed
InCommand	v1.0 - 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42	CyberNotes-2000-09
Infector	v1.3	CyberNotes-2000-07
iniKiller	v1.2 - 3.2 Pro	CyberNotes-2000-10
iniKiller	v1.2 - 3.2	CyberNotes-2000-09
Intruder		CyberNotes-2000-01
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Kuang Original	0.34	CyberNotes-2000-01
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0	CyberNotes-2000-01
Matrix	v1.0 - 2.0	CyberNotes-2000-09
MoSucker		CyberNotes-2000-06
Naebi	v2.12 - 2.39	CyberNotes-2000-09
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
NetTrojan	1.0	CyberNotes-2000-06
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	1.2-1.3	CyberNotes-2000-06
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65	CyberNotes-2000-09
Setup Trojan (Sshare) +Mod Small Share		CyberNotes-2000-06
ShadowPhyre	v2.12.38 - 2.X	CyberNotes-2000-06
ShitHeap		CyberNotes-2000-09
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Trinoo		CyberNotes-2000-05
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05
WinCrash	**Beta**	**Current Issue**

GIP (May 22, 2000): Another name for the Trojan is reportedly price.doc.exe. This Trojan will steal and e-mail changed passwords via SMTP back to the configured destination. The Trojan has several configurable parameters including the frequency of e-mailings. The program installs iteself into the %SYSTEMROOT% directory. It will make changes to the registry to be able to run at startup. This Trojan is hosted on a Russian website with an English translation and also claims to connect back to the hosting site and update itself when new releases become available.

WINCRASH.B (May 24, 2000): This Trojan has been reported in the wild. This new backdoor, remote control Trojan is similar to well known Trojans such as Netbus, SubSeven, and BackOrifice. The Trojan is used to remote control a PC. It has both a client and a server.

There is a dropped file, names Register.exe, which most antivirus software can detect as JOKE_FLIPPED, that causes the screen display to flip. Msdecay.scr is set to be the default screen saver, which shows a melting screen. The other files are used by the server program as its component files to ensure proper execution.

The Trojan puts a copy of itself as SERVER.EXE in the Windows folder. The Trojan then modifies WIN.INI by adding the following line: run=drive:\Windows\SERVER.EXE. The program will then execute every startup. The server program is the program that allows the malicious user to connect to the remote PC. The server program, when run, puts the following files in the Windows\System folder:

Msvsrv.exe- 26,112 bytes
Mdihole.exe – 6,146 bytes
Redire32.exe- 31,744 bytes
Register.exe - 4,128 bytes
Msdecay.scr 20,992 bytes

The client program of the Trojan can be used to manipulate the computer of the victim running the server program. This client program enables the malicious user to perform such actions as:

- Control external devices – keyboard, mouse, printer, monitor, and CD-ROM.
- Control windows – taskbar, start button
- Get system information about the server
- Shut down or disconnect from the server

ICQ PWS (May 24, 2000): This Trojan is an adaptation of the 7sphere port scanner from April, 1997. The program specifically focuses on ICQ passwords.